CLAIMS:

1. A method for controlling distribution and use of a digital work (DW), comprising the steps of:

a) attaching a usage right information to said digital work (DW), said usage write information defining one or more conditions which must be satisfied in order for said usage right to be exercised;

b) storing said digital work (DW) and its attached usage right information on a record carrier (10);

c) updating said attached usage right information with every use of said digital work (DW); and

d) refusing the use of said digital work if said usage right information indicates that the usage right has been exercised;

characterized in that

e) a hidden information (KLK) stored in a hidden channel and used for encrypting or verifying said usage right information is changed when said usage right information has changed.

2. A method according to claim 1, characterized in that said hidden information is a checksum over a data block containing said usage right information.

3. A method according to claim 1, characterized in that said hidden information is a key (KLK) used for decrypting said usage right information, wherein said key is randomly changed and said usage right information is re-encrypted by using said changed key, when said usage right information has changed.

4. A method according to claim 3, characterized in that the previous key (KLK-1) is destroyed after the change of said key.

5. A method according to any of claims 1 to 3, characterized in that said hidden channel is arranged to be not accessible by commercial reproducing devices.

6. A method according to claim 5, characterized in that said hidden channel is generated by:

- storing said hidden information (KLK) in deliberate errors which can be corrected again;
- storing said hidden information (KLK) in merging bits of a runlength-limited code;
- controlling a polarity of predetermined runlength of a predetermined word of a runlength-limited code according to said hidden information (KLK);
- storing said hidden information (KLK) in deliberate errors in a time-base; or
- storing said hidden information (KLK) in a memory embedded with a disc controller.

7. A method according to any of claims 2 to 6, characterized in that said attached usage right information is stored in a table (KLT) together with a key information used for decrypting said digital work (DW).

8. A method according to any of claims 1 to 7, characterized in that said digital work (DW) is an audio track downloaded from the Internet, and said record carrier is a recordable optical disc, a hard disc, a magneto-optic recording device, a magnetic tape, or a memory card.

9. A method according to any of claims 1 to 8, characterized in that said usage right information comprises a counter information which can be updated when said usage right has been exercised.

10. A method according to any of claims 1 to 9, characterized in that each track of said recording medium (10) comprises its own usage right information and hidden information (KLK).

11. A record carrier for storing a digital work (DW) and a usage right information defining one or more conditions which must be satisfied in order for the usage right to be exercised, characterized in that said recording carrier (10) comprises a hidden channel which is not accessible by a commercial reproducing devices and in which a hidden information (KLK) is stored which is used for encrypting or verifying said usage right information and which is changed when said usage right information has changed.

12. A record carrier according to claim 11, characterized in that said record carrier is a recordable optical disc (10), in particular a CD or a DVD.

13. A device for controlling distribution and use of a digital work, comprising:

a) writing means (20) for writing said digital work (DW) and an attached usage right information defining one or more conditions which must be satisfied in order for the usage right to be exercised, on a record carrier (10);

b) updating means (22) for updating said attached usage right information with every use of said digital work; and

c) control means (21) for refusing the use of said digital work (DW) if said updated usage right information indicates that the usage right has been exercised

characterized in that

d) said updating means (22) is arranged to change a hidden information (KLK) stored in a hidden channel and used for encrypting or verifying said usage right information, when said usage right information has changed.